(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2003 (05.06.2003)

PCT

(10) International Publication Number
WO 03/046842 A1

(51) International Patent Classification[7]: G07D 11/00, B32B 27/36

(21) International Application Number: PCT/GB02/05259

(22) International Filing Date:
22 November 2002 (22.11.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

0128176.5	23 November 2001 (23.11.2001)	GB
0216879.7	19 July 2002 (19.07.2002)	GB
0216878.9	19 July 2002 (19.07.2002)	GB

(71) Applicant *(for all designated States except US)*: **DE LA RUE INTERNATIONAL LIMITED** [GB/GB]; De La Rue House, Jays Close, Viables, Basingstoke, Hampshire RG22 4BS (GB).

(72) Inventors; and

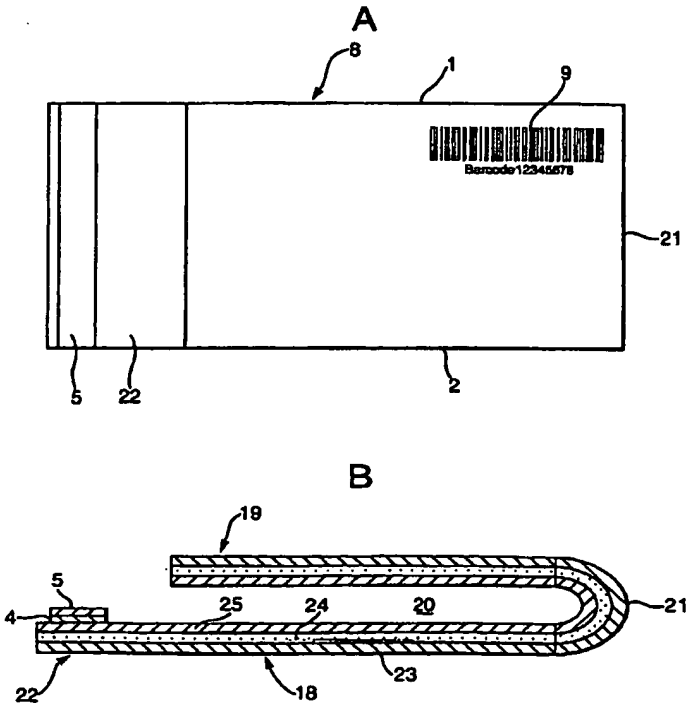
(75) Inventors/Applicants *(for US only)*: **IRELAND, Phillip, Michael, William** [GB/GB]; 2 Mallard Road, Rowlands Castle, Hampshire PO9 6HE (GB). **JAMES, Alexander, Charles, Harold** [GB/GB]; 102 Stakes Road, Waterlooville, Hampshire PO7 5PB (GB). **CUNNINGHAM, Karen, Joan** [GB/GB]; 11 Station Rise, Marlow, Buckinghamshire SL7 1EJ (GB). **ARMANINI, Pietro** [IT/GB]; Marjoram Cottage, Preston Candover, Herts RG25 2EE (GB). **CALVERLEY, Simon, George** [GB/GB]; 63 Victory Avenue, Horndean, Hants PO8 9PJ (GB). **POTTER, Michael** [GB/GB]; Pidham Cottage, Langrish, Near Petersfield, Hampshire GU32 1RN (GB).

(74) Agent: **GILL JENNINGS & EVERY**; Broadgate House, 7 Eldon Street, London EC2M 7LH (GB).

[Continued on next page]

(54) Title: TAMPER EVIDENT CONTAINER

(57) Abstract: A tamper evident container (8), the walls (23-25) of which have a machine detectable tamper evident structure such that tampering with substantially any part of the container can be detected.



WO 03/046842 A1

(81) **Designated States** *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TAMPER EVIDENT CONTAINER

The present invention relates to tamper evident containers for items of value such as banknotes and coins and a method for inspecting the physical integrity of such containers.

It is known to transport items of value in secure tamper evident containers. Items of value in this instance include but are not limited to banknotes, cheques, fiscal stamps, stamps, scratch cards, certificates of authenticity, brand protection items, secure labels, and casino chips. In general, the present invention could be used in any application where a user wishes to transport a valuable item via relatively insecure means and/or though an insecure environment.

Within the prior art a wide variety of tamper evident containers have been disclosed for transporting items of the type described above. For example, a closure device or a label applied onto the container/closure is often used to indicate tampering.

It is also known to provide machine authenticable devices on tamper evident packaging and containers, some of which will be destroyed upon opening of the package but these are limited in their benefit. Typically such devices are applied as a label and/or located in the region of a closure such as a flap, clasp or zip fastener. Upon opening the closure the device is destroyed or altered in some way so as to modify the response to its associated detection apparatus. One major limitation is that it is assumed that someone will attempt to enter the envelope via the normal route, namely the envelope flap. If someone were to enter the envelope by any other route this would not be detected by the automated process.

In accordance with a first aspect of the present invention, a tamper evident container is provided, the walls of which have a machine detectable tamper evident

structure such that tampering with substantially any part of the container can be detected.

The current invention overcomes these problems by firstly providing the entire container with the means to indicate tampering, and secondly enabling any attempt to tamper with the product to be determined by automatic inspection.

The container can take a variety of forms and could comprise a rigid or semi-rigid container of metal or plastics (typically mechanically or electronically locked). The use of a secure cassette for banknotes is advantageous since the notes can then be automatically fed into document sorting equipment at the financial institution. However, the invention is particularly concerned with flexible containers made, for example, of paper or plastics and including in particular, envelopes.

A number of different types of machine detectable tamper evident structures have been developed.

In a first example, the container walls are formed by a laminate structure, each layer of the laminate luminescing, for example fluorescing, with a different, visible colour under non-white and/or non-visible light illumination, the outer layer being opaque at least under white light illumination.

This is particularly convenient for detecting tampering using a simple irradiation technique, typically UV irradiation. If a luminescent, e.g. fluorescent, wavelength is detected which would not be expected in the normal course from a container which had not been tampered with, then this will indicate possible tampering enabling the system to refuse to accept the container.

In a second example, the machine detectable tamper evident structure is in the form of one or more resonant, electrical circuits. On tampering, one of these circuits will be broken and this can be easily detected using suitable detection equipment.

In addition to its tamper evidence, the container may include on or inside it a code at least identifying the container and preferably relating to the content of the container.

In some cases, the code could be printed on the container just before, during or even after the items of value have been inserted into the container. In another option, the container is provided with a transparent region and contains a code carrier, for example a receipt, printed at the time the container was filled, providing the code such as a bar code, which can be read through the transparent portion. In a further option, the container is opaque but contains a storage device, e.g. a RFID or EAS, whose content can be read through the container wall. In either case, a further identification label could be placed on the outside of the container.

The use of a code provides a means by which data can be associated with the container. Such data may comprise information relating to the contents of the container, point of origin, intended destination, time of filling, expected time of arrival, and identity of the sender. Details of the potential applications for a container conforming to the current invention and having data associated with it can be found in our co-pending International Applications of even date entitled "Improvements Relating to Depositing Items of Value" (Agents Ref: RSJ07156WO) and "Verification Method and Apparatus" (Agents Ref: RSJ07663WO).

Further security features such as security threads, security print and the like could also be provided on or in the container as will be described in more detail below.

Tamper evident containers can be used simply to store items of value in a secure manner but have particular application for transferring items of value from one location to another. This also enables account information to be changed to reflect transfer of ownership of items of value without the need to open the container.

In accordance with a second aspect of the present invention, a method of detecting tampering of a container according to the first aspect of the present invention comprises irradiating the container with electromagnetic radiation at working wavelengths so as to detect a change in the tamper evident structure.

In the case of the laminate structure, the electromagnetic radiation will typically comprise UV or infrared radiation while in the case of resonant circuits, the electromagnetic radiation will typically comprise RF radiation in the range 1-20MHz.

Some examples of containers and apparatus for carrying out methods according to the invention will now be described with reference to the accompanying drawings, in which:-

Figures 1A and 1B are a plan and schematic cross-section respectively through a first example of a tamper evident envelope;

Figure 2 is a block circuit diagram illustrating an example of apparatus for determining the physical integrity of the container shown in Figures 1A and 1B;

Figures 3A and 3B illustrate a second example of an envelope according to the invention and a single resonant circuit respectively; and,

Figure 4 is a plan view of an envelope constructed according to any of the previous examples and carrying a number of additional security features.

For the sake of clarity the examples below refer to transporting banknotes but the containers could, In principle be used for any items of value as previously defined.

The tamper evident envelope 8 shown in Figures 1A and 1B can be constructed in a variety of ways, one of which is shown. Figure 1A illustrates the envelope 8 in its unsealed condition having a lower leaf 18 secured along edges 1,2 (by pressure sensitive or, preferably heat seal adhesive) to an upper leaf 19 and defining a space 20

therebetween. In practice, the leaves 18,19 may be formed by simply folding a single laminate about a line 21. As shown in Figures 1A and 1B the lower leaf 18 defines a flap portion 22 carrying a self-adhesive strip 4 having a cover strip 5 pre-applied so notes/documents inserted into the envelope do not attach themselves when the envelope is filled. The adhesive used for the strip 4 and between the leaves 18,19 will achieve a bond strength greater, that is higher, than achieved within the triple layers of the envelope material (to be described). This is to ensure that unauthorised opening can be detected. Examples of suitable adhesives are HB-Fuller SE5235, SE5269 which are water based or Ashland Adhesives 390M which is solvent based. The adhesive SE5235 could also be used as a pressure sensitive adhesive for the sealing of laminate envelopes. After documents have been inserted into the envelope 8, the strip 5 is removed, and the flap portion 22 folded over and adhered to the upper leaf 19. Any conventional means can be used to achieve automatic folding and sealing. The sealed envelope can now be handled in a relatively unsecure manner which is particularly advantageous.

In this example the envelope 8 has also been coded, using a barcode 9, in such a way that its content can be identified without opening the container. In this instance the code is pre-printed onto the container so as uniquely to identify the container, the code enabling a store or memory to be addressed which contains information defining, amongst other things, the total value of the contents.

Typically, details of the barcode 9 will be stored in a central database or host. Within the database additional data may be associated with the code, such information may define the value and denomination split of the banknotes contained therein or other pertinent data such as from where the banknotes originated, the time and place the envelope was filled and the destination and expected arrival time of the envelope.

Each leaf 18,19 is made up of a triple laminate of layers 23-25 respectively. Each layer 23-25 comprises a polyester material containing titanium dioxide so that it presents a white, opaque colour under normal, white light illumination, each layer then being provided with a different fluorescent additive. The layer 23 has an orange fluorescent additive, the layer 24 a green fluorescent additive, and the layer 25 a yellow phosphorescent additive. Suitable additives can be obtained from Imperial Materials.

Under non-white light, eg UV, illumination the layers 23-25 will fluoresce in accordance with their particular additives. If the envelope 8 has not been tampered with then only the outer, orange fluorescence will be visible. If, however, an attempt has been made to scratch information from the surface of the envelope or to cut the envelope, there will be a change in the resultant visible fluorescence which can be detected. In some cases, damage could be detected using visible irradiation, for example if a brightly coloured material is exposed and this is visible in normal light.

In order to be able to handle envelopes of the type shown in Figures 1A and 1B, a bar code and tamper evident reader system 16 is constructed as shown in Figure 2. The system comprises two pairs of feed rollers 30,31 controlled by a motor 32 which in turn is controlled from a microprocessor 33. Upper and lower UV sources 34,35 controlled from the microprocessor 33 are provided downstream of the rollers 30, and sensors 36,37 are located downstream of the sources 34,35 to detect fluorescent light.

A pair of white light sources 38,39 are located downstream of the sensors 36,37 for the purpose of detecting a bar code 9, reflected light being incident on respective sensors 41,42 connected to the microprocessor 33.

When an envelope 8 is presented to the input (not shown) of the reader system 16, it is detected by a sensor (not shown) to which the microprocessor 33 responds by activating the rollers 30,31 to draw the envelope 8 into the system. The microprocessor 33 then activates the sources 34,35 which like the other sources and detectors extends across the full width of the envelope 8 so that the envelope is irradiated with UV radiation on both sides. Any fluorescent radiation will be received through suitable filters by the sensors 36,37 and the intensity of this radiation together with wavelength information will be fed to the microprocessor 33.

The microprocessor 33 then compares the received wavelengths and possibly the locations on the envelope generating the received wavelengths with prestored information in a store 43. This prestored information may comprise wavelengths which would be detected if the envelope had been tampered with, optionally with this information being stored for each region of the envelope monitored by the sensors 36,37. If any radiation is received which suggests that the envelope has been tampered with (in the example described above this would correspond to green or yellow radiation) then the microprocessor 33 will determine that the envelope has been tampered with and cause the motor 32 to reverse so that the envelope is fed back out of the input slot. It will be appreciated that the structure of the envelope is such that tampering with any part of it will be detected.

If the tamper evident test is successful, the white light sources 38,39 are illuminated so that the bar code information can be sensed by one of the sensors 41,42 and be passed to the microprocessor 33. The microprocessor 33 then allows the envelope 8 to be fed onto a store (not shown) while transmitting information about the bar code to a remote host so that the host can credit an account with the value of the items e.g. banknotes in the envelope without the need to open the envelope.

In simpler forms of the apparatus, only one side of the envelope could be inspected. If unsuccessful, the user would then need to insert the envelope in a different orientation to be checked again.

Also, under controlled conditions, the envelope could be manually scanned and in this case it is preferable to apply bar codes in multiple positions down each side of the envelope so that to achieve deposit the detector must see all the bar codes and hence have a reasonable view of the complete exterior of the envelope.

In a second example tamper evidence is provided by conductive tracks printed onto an inner layer of the material with connection pads that enable the integrity of the circuits to be checked. It is then possible to detect if the tracks are cut or broken. Conductive adhesives could also be used across the seal area. In another possibility, aerials could be printed on an inner layer of the package or envelope. The aerials can be energised remotely, e.g. with a coil, and a resonance frequency measured. If the aerial has been damaged by breaking or cutting then either no or an incorrect resonance frequency will be returned. Each envelope or package may have one or more aerials, possibly with different resonant frequencies.

A second example of a tamper evident structure is shown in Figures 3A and 3B. This could be used alone or in combination with the first example. The basic idea is to provide for a number (eight are shown in Figure 3A) of resonant circuits (one shown in Figure 3B), nominally identical, and placed close together in a row that completely covers the sealed area defined within a sealed package.

The edges of the foil or conductive ink tracks are narrower than usual, and are wavy, rather than straight, as is normal in EAS applications. The gap between adjacent circuits is small. This makes it very difficult to make a cut of a size suitable for removing banknotes from the package without cutting a track. It may be possible to use

a common track for two or more of the circuits, making it impossible to make a cut without cutting a circuit track. Typically, the resonant circuit(s) will cover the whole of the surface of the container/envelope, in order to prevent cuts being made that are big enough to remove the contents without detection.

The top and bottom parts of the package may be multi-layer, with the resonant circuit tag layers on the inside, and thicker layers on the outside. This will help to disguise the exact positions of the resonant circuits.

The package is made of two similar parts (not shown), the top and the bottom, that are securely stuck together. The adhesive and substrate are chosen such that any attempt to split the adhesive results in a tearing of the substrate and the circuits. (The top and bottom may be on the same substrate if it is easier to form the package by folding a single sheet.)

The resonant frequencies of the circuits on the top are different from those on the bottom.

The integrity of the circuits can be detected by a pair of relatively short-range detectors (not shown), mounted on for example a letterbox slot or a handheld device. The package is passed between the detectors which describe a detector track along the package. The detector will emit RF radiation in the frequency range of, typically, between 1 and 20MHz and will normally be scanned through all or part of the range. The introduction of the tuned circuits would modify the radiation output, increasing it at the resonant frequency/ies of the tuned circuit/s, causing peaks in the response. The frequency at which the circuit/s resonate can be measured and verified to ensure that it/they is/are indeed the correct frequency/ies for that package. The circuits could be designed to resonate at different frequencies such that the detected frequencies form a "code" for that particular package or type of package.

Normally, both detectors will find the correct number of circuits on the package; any tampering will cause at least one circuit to be destroyed (or at least severely disturbed).

For both of the above examples additional security and/or tamper evident features may be provided on or in the substrate of the package/envelope as indicated in Figure 4. Features that may be included in the substrate include partially or wholly embedded security threads 50, watermarks 51, planchettes, security fibres, and machine detectable additives. Such features may also be treated so as to react to heat and solvent attack such as might be used by someone attempting to remove an adhesive layer. The package may also be provided with other overt and covert security features on its outer surface. Such surface features include security print 52, diffractive optically variable devices (DOVIDs) 53, optically variable inks and layers (e.g. OVI®, iridescent inks, pearlescent inks, liquid crystal layers), intaglio print, latent image devices, functional layers (e.g. thermochromics, photochromics, luminescent materials, magnetic inks and materials and taggants). Again surface features and inks may be provided so as to react to various forms of attack such as heat and solvent. Such devices be they included in or on the substrate provide an additional level of security that can be interrogated to determine the authenticity of the package.

CLAIMS

1. A tamper evident container the walls of which have a machine detectable tamper evident structure such that tampering with substantially any part of the container can be detected.

2. A container according to claim 1, wherein the container is in the form of an envelope having a flap which can be folded over and sealed to a wall of the envelope.

3. A container according to claim 1 or claim 2, wherein the walls are made of paper and/or plastics.

4. A container according to any of the preceding claims, wherein the container walls are formed by a laminate structure, each layer of the laminate luminescing, for example fluorescing, with a different, visible colour under non-white and/or non-visible light illumination, the outer layer being opaque at least under white light illumination.

5. A container according to claim 4, wherein the layers of the laminate luminesce, e.g. fluoresce, under UV illumination.

6. A container according to claim 4 or claim 5, wherein the outer layer is white under white light illumination.

7. A container according to any of the preceding claims, wherein the machine detectable tamper evident structure comprises one or more resonant, electrical circuits.

8. A container according to any of the preceding claims, wherein the container carries or includes a code related to the content of the container.

9. A container according to claim 8, wherein the code is provided on an outer surface of the container.

10. A container according to any of the preceding claims, further comprising one or more additional security features chosen from partially or wholly embedded security threads, watermarks, planchettes, security fibres, and machine detectable additives, security print, diffractive optically variable devices (DOVIDs), optically variable inks and layers (e.g. OVI®, iridescent inks, pearlescent inks,

liquid crystal layers), intaglio print, latent image devices, and functional layers (e.g. thermochromics, photochromics, luminescent materials, magnetic inks and materials and taggants).

11. A method of detecting tampering of a container according to any of the preceding claims, the method comprising irradiating the container with electromagentic radiation at working wavelengths so as to detect a change in the tamper evident strucutre.

12. A method according to claim 11, when dependent on claim 7, wherein the electromagnetic radiation causes untampered resonant, electrical circuits to resonate.

13. A method according to claim 11, when dependent on any of claims 4 to 6, wherein the electromagnetic radiation causes fluorescence within each layer of the laminate.

Fig.1A.

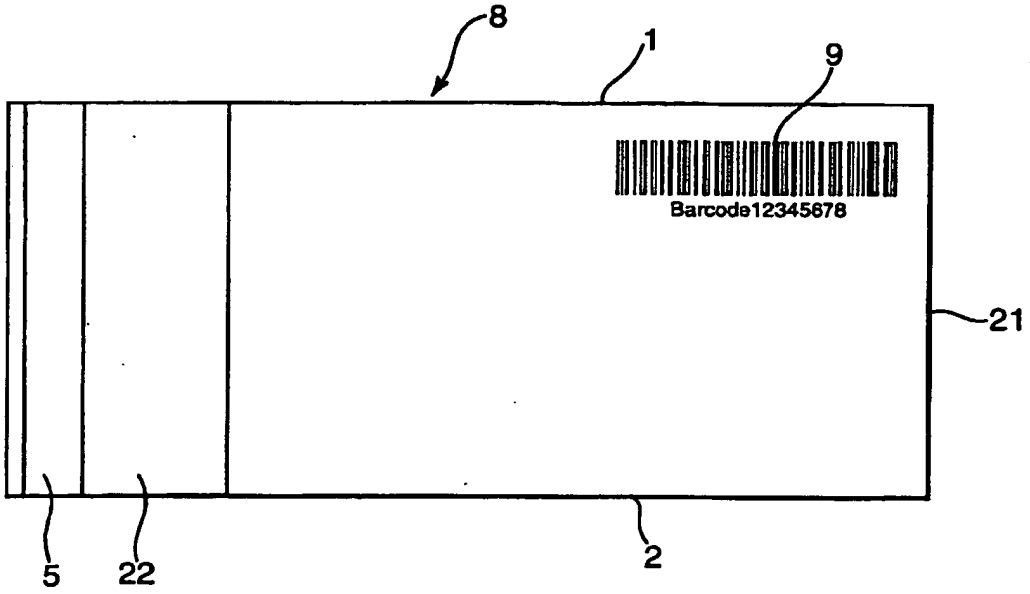
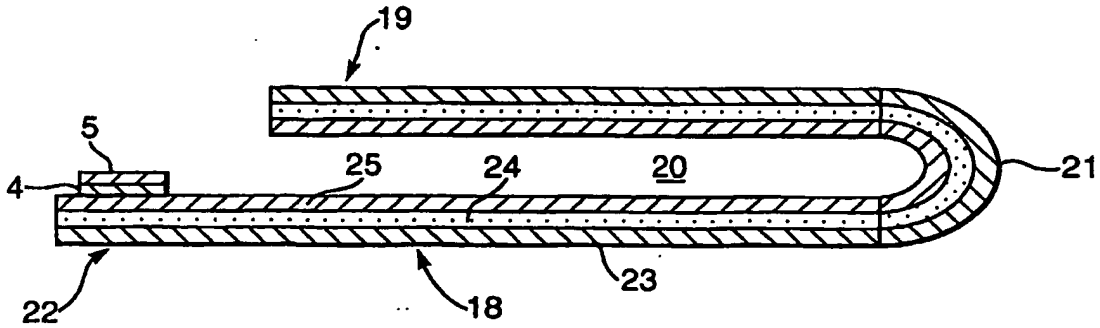


Fig.1B.



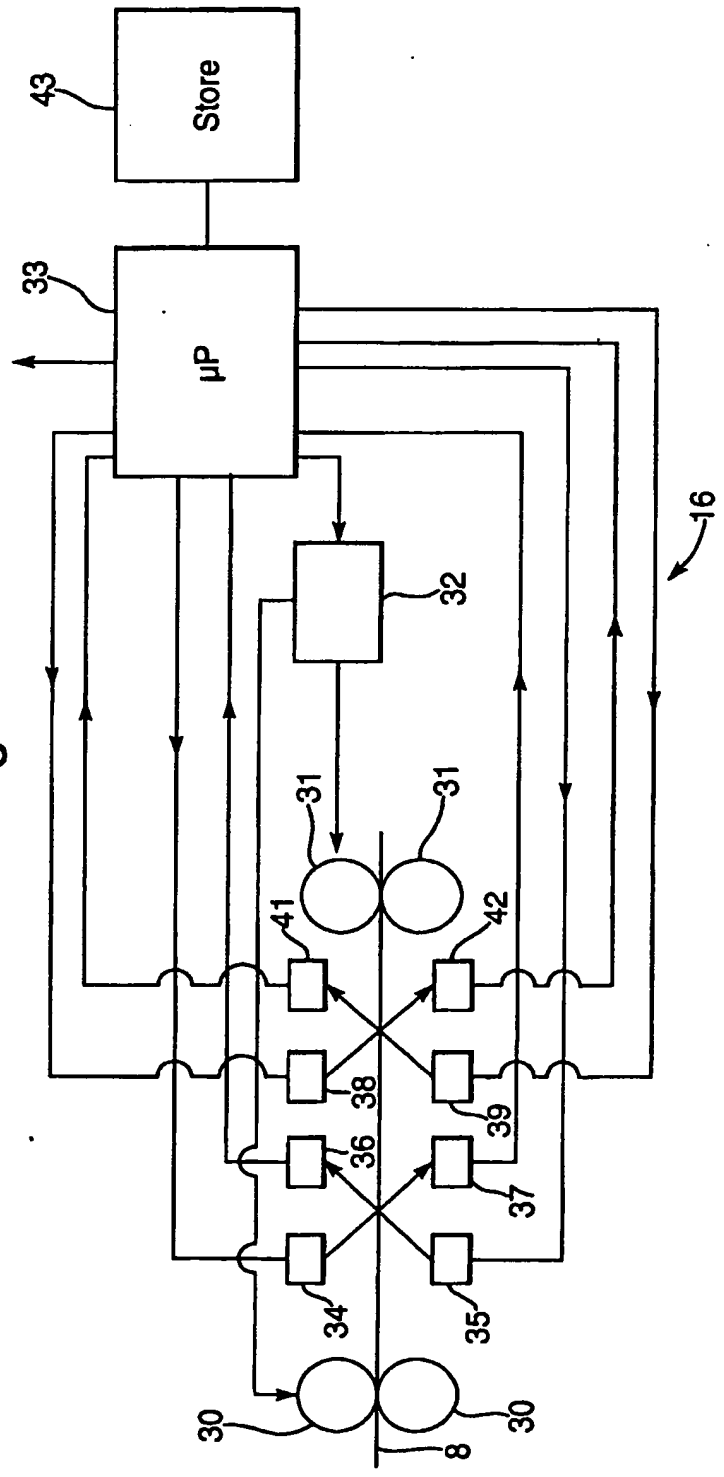


Fig.2.

Fig.3A.

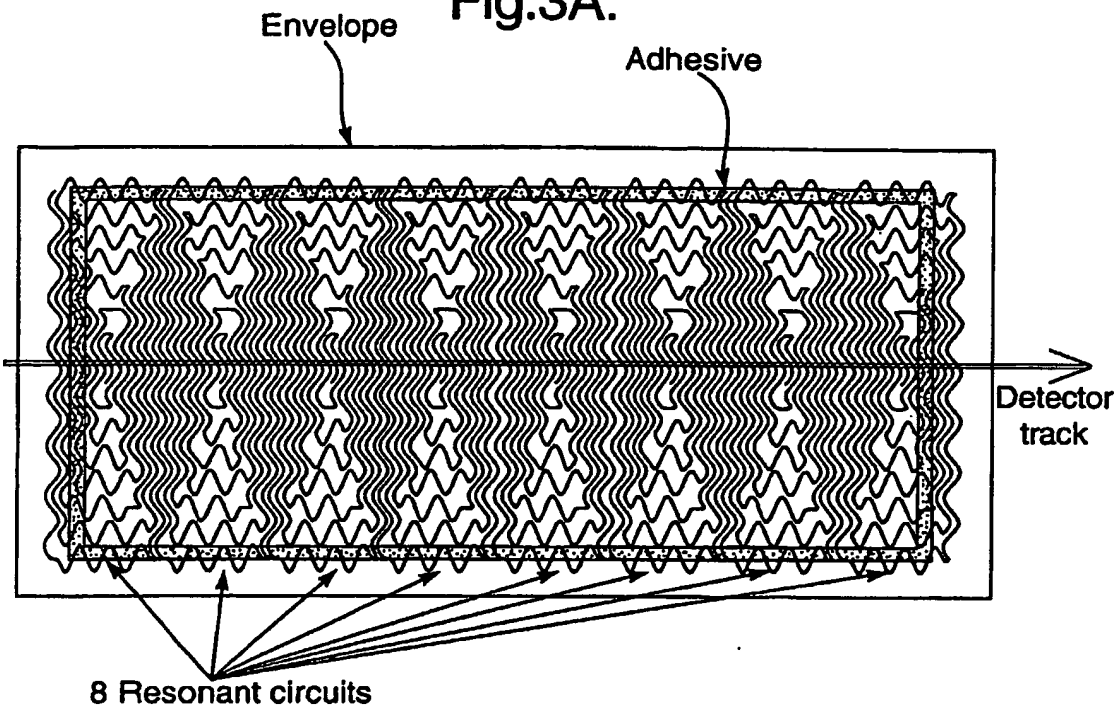

Envelope
Adhesive
Detector track
8 Resonant circuits

Fig.3B.

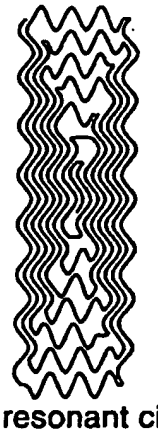
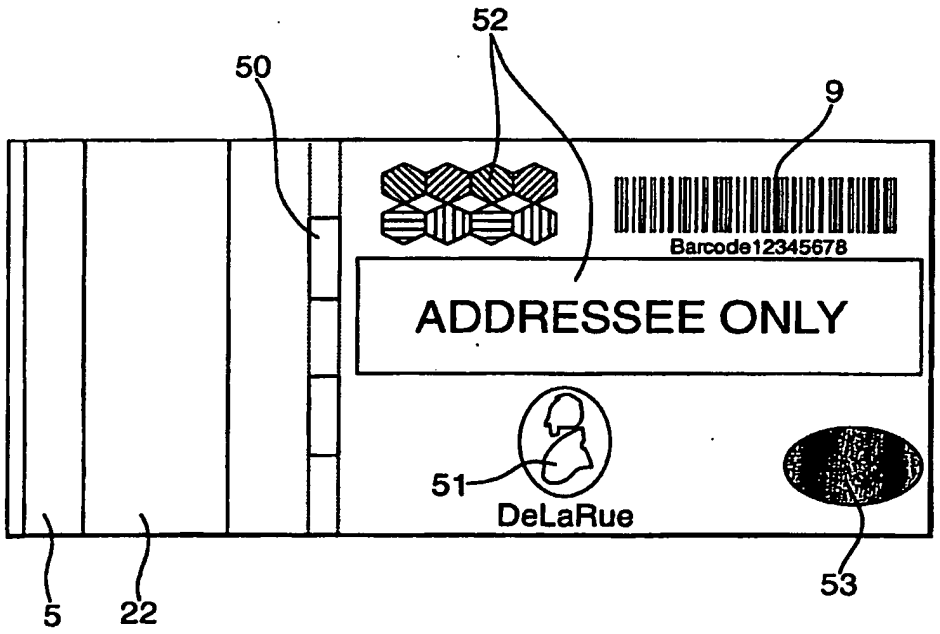

Single resonant circuit

Fig.4.



INTERNATIONAL SEARCH REPORT

PCT/GB 02/05259

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07D11/00 B32B27/36

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07D B32B E05G G08B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 6 215 397 B1 (LINDSKOG KJELL) 10 April 2001 (2001-04-10) abstract figures 1,3,4 column 2, line 25 - line 31 column 3, line 12 - line 20	1,3,7,10 8,9
A	US 5 992 891 A (DYBALL CHRISTOPHER J) 30 November 1999 (1999-11-30) abstract column 1, line 43 - line 56	1,4,5, 11,13
Y	EP 1 031 949 A (NCR INT INC) 30 August 2000 (2000-08-30) abstract column 2, line 24 - line 35	8,9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 February 2003	21/02/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Verhoef, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

PCT/GB 02/05259

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6215397 B1	10-04-2001	US 6400268 B1	04-06-2002
US 5992891 A	30-11-1999	NONE	
EP 1031949 A	30-08-2000	EP 1031949 A1	30-08-2000